PBGC
Protecting America's Pensions

OFFICE OF INSPECTOR GENERAL
AUDIT REPORT

Pension Benefit Guaranty Corporation's Fiscal Year 2018 Compliance with the Federal Information Security Modernization Act of 2014

Report No. AUD-2019-04
December 20, 2018

December 20, 2018

TO: Thomas Reeder
Director

FROM: Brooke Holmes
Assistant Inspector General for Audits, Evaluations, and Reviews

SUBJECT: Issuance of Final Report No. AUD-2019-04/FA-18-127-4
Pension Benefit Guaranty Corporation's Fiscal Year 2018 Compliance with the Federal Information Security Modernization Act of 2014

I am pleased to transmit the Pension Benefit Guaranty Corporation's Fiscal Year 2018 Compliance with the Federal Information Security Modernization Act of 2014 (FISMA) audit report detailing the results of our review of the PBGC information security program.

As prescribed by FISMA, the PBGC Inspector General is required to conduct annual evaluations of the PBGC security programs and practices, and to report to the Office of Management and Budget the results of this evaluation. CliftonLarsonAllen LLP, on behalf of the OIG, completed the OMB-required responses that we then submitted to OMB. This year, CliftonLarsonAllen LLP issued ten new FISMA-related recommendations. Five were issued in the Financial Statements audit report and five are issued in this report. PBGC agreed with the five new recommendations in this report and previously agreed with the five recommendations in the Financial Statements audit report.

We would like to take this opportunity to express our appreciation for the overall cooperation CliftonLarsonAllen LLP and OIG received during this audit.

cc: Robert Scherer, Chief Information Officer
Patricia Kelly, Chief Financial Officer
Alice Maroni, Chief Management Officer
Karen Morris, Chief of Negotiations and Restructuring
Michael Rae, Deputy Chief Policy Officer
Judith Starr, General Counsel
Marty Boehm, Director, Corporate Controls and Reviews Department

The Audit of the Pension Benefit Guaranty Corporation's Compliance with the Federal Information Security Modernization Act of 2014

Fiscal Year 2018

December 18, 2018

CliftonLarsonAllen LLP
CLAconnect.com

December 18, 2018

Robert A. Westbrooks
Inspector General
Pension Benefit Guaranty Corporation
1200 K Street, NW
Washington, DC 20005-4026

Dear Mr. Westbrooks:

CliftonLarsonAllen LLP is pleased to present our report on the Pension Benefit Guaranty Corporation's (PBGC) compliance with the Federal Information Security Modernization Act of 2014 (FISMA).

We appreciate the assistance we received from PBGC and appreciate the opportunity to serve you. We will be pleased to discuss any questions or concerns you may have regarding the contents of this report.

Very truly yours,

Sarah Mirzakhani, CISA
Principal

CliftonLarsonAllen LLP
CLAconnect.com

Inspector General
Pension Benefit Guaranty Corporation

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the Pension Benefit Guaranty Corporation's (PBGC) compliance with the Federal Information Security Modernization Act of 2014 (FISMA). The objective of this evaluation was to determine the extent to which the PBGC's information security program and practices complied with FISMA requirements, Department of Homeland Security (DHS) reporting requirements, and applicable Office of Management and Budget (OMB) and National Institute for Standards and Technology (NIST) guidance. The audit included the testing of selected management, technical, and operational controls outlined in NIST's Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

For this audit, we reviewed selected controls for six of PBGC's internal and external information systems. We performed audit fieldwork at the PBGC's headquarters in Washington, D.C., during the period April 2018 through November 2018.

The audit was performed in accordance with the performance audit standards specified in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

There are five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.0. According to the objective evaluation metrics of the Framework, PBGC's security program, as in the prior year, fell below the specified threshold of effectiveness, which is level 4, *Managed and Measurable*. We did note areas of improvement in FY 2018. One functional area, *Respond*, was found to meet the *Managed and Measurable* (Level 4) requirements.[1] Prior year weaknesses in Contingency Planning were also remediated during FY 2018.

We also concluded that PBGC did not implement an effective information security program for many of the selected security controls for selected information systems. PBGC's implementation of a subset of selected controls was not fully effective to ensure the confidentiality, integrity, and availability of the Corporation's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, CLA noted weaknesses in 7 of the 8 Inspector General FISMA Metric Domains and have made a total of 10 new, and 16 repeated or modified recommendations to assist PBGC in strengthening its information security program.

[1] The most frequent maturity level rating across the Protect function served as the overall Protect function rating.

Additional information on our findings and recommendations are included in the accompanying report.

CliftonLarsonAllen LLP

Greenbelt, Maryland
December 18, 2018

Table of Contents

Executive Summary

The Federal Information Security Modernization Act of 2014 (FISMA) requires agencies to adopt a risk-based, life-cycle approach to improve computer security, which includes annual security program reviews, independent evaluations by the Inspector General (IG), and reporting to the Office of Management and Budget (OMB) and the Congress. It also codifies existing policies and security responsibilities outlined in the Computer Security Act of 1987 and the Clinger Cohen Act of 1996.

The Pension Benefit Guaranty Corporation (PBGC or the Corporation) Office of Inspector General (OIG) engaged CliftonLarsonAllen LLP (CLA) to conduct an audit in support of the FISMA requirement for an annual evaluation of PBGC's information security program. The objective of this performance audit was to determine the extent to which the PBGC's information security program and practices complied with FISMA requirements, Department of Homeland Security (DHS) reporting requirements, and applicable OMB and National Institute for Standards and Technology (NIST) guidance.

The FISMA evaluation requires us to assess the maturity of five functional areas in PBGC's information security program.[2] This assessment used objective metrics that are standardized across the federal government. To be considered effective, an agency's IT security must be rated *Managed and Measurable* (Level 4), on a five-point scale from *Ad hoc* (Level 1) to *Optimized* (Level 5). PBGC did not reach that level. Four of the five functional areas at PBGC achieved a maturity level of *Consistently Implemented* (Level 3). One function, *Respond*, was found to be *Managed and Measurable* (Level 4).

PBGC took corrective actions on information technology (IT) recommendations from our financial statement internal control reports and prior FISMA reports; however, based on the weaknesses identified and the continued existence of unremediated recommendations, we conclude that PBGC's information security program still needs improvement. Specifically, CLA noted weaknesses in risk management, vulnerability and configuration management, identity and access management, data protection and privacy, security training, and information security continuous monitoring.

To address these weaknesses, we made a total of 10 new, and 16 repeated or modified recommendations to assist PBGC in strengthening its information security program.

[2] The FY 2018 metrics are based on a maturity model approach begun in prior years and align the metrics with all five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.0: Identify, Protect, Detect, Respond, and Recover.

Background

Corporation Overview

The Corporation protects the pensions of more than 37 million workers and retirees in more than 25,000 plans. Under Title IV of the Employee Retirement Income Security Act of 1974, PBGC insures, subject to statutory limits, pension benefits of participants in covered private defined-benefit pension plans in the United States. To accomplish its mission and prepare its financial statements, PBGC relies extensively on the effective operation of information technology. Internal controls are essential to ensure the confidentiality, integrity, and availability of critical data while reducing the risk of errors, fraud, and other illegal acts.

PBGC has become increasingly dependent on computerized information systems to execute its operations and to process, maintain, and report essential information. As a result, the reliability of computerized data and of the systems that process, maintain, and report this data are major priorities for PBGC. Although the increase in computer interconnectivity has changed the way the government does business, it has also increased the risk of loss and misuse of information by unauthorized or malicious users. Protecting information systems continues to be one of the most important challenges facing government organizations today.

FISMA Legislation

The Federal Information Security Modernization Act of 2014[3] (FISMA) provides a comprehensive framework for ensuring effective security controls over information resources supporting federal operations and assets. FISMA requires federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source.

The statute also provides a mechanism for improved oversight of federal agency information security programs. FISMA requires agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capability is established, and (3) information security management processes are integrated with the agency's strategic and operational planning processes. All agencies must also report annually to OMB and to congressional committees on the effectiveness of their information security program.

Federal agencies are to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by the agency. As specified in FISMA, the agency Chief Information Officer (CIO) or senior official is responsible for overseeing the development and maintenance of security operations that continuously monitor and evaluate risks and threats.

FISMA also requires agency Inspector Generals (IGs) to assess the effectiveness of agency information security programs and practices. Guidance has been issued by OMB and by NIST (in its 800 series of Special Publications) supporting FISMA implementation. In addition, NIST issued

[3] The Federal Information Security Modernization Act of 2014 (Public Law 113–283—December 18, 2014) amends the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices and (2) set forth authority for the Secretary of the Department of Homeland Security to administer the implementation of such policies and practices for information systems.

the Federal Information Processing Standards (FIPS) to establish agency baseline security requirements.

FY 2018 IG FISMA Reporting Metrics

OMB and DHS annually provide instructions to federal agencies and IGs for preparing FISMA reports. On October 16, 2017, OMB issued Memorandum M-18-02, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements*. This memorandum describes the processes for federal agencies to report to OMB and, where applicable, DHS. Accordingly, the *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, provided reporting requirements across key areas to be addressed in the independent assessment of agencies' information security programs.[4]

The FY 2018 metrics are based on a maturity model approach begun in prior years and align the five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.0: Identify, Protect, Detect, Respond, and Recover. Data Protection and Privacy was added to the FY 2018 metrics in the Protect security function. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IGs with a method for assessing the maturity of controls to address those risks, as highlighted in **Table 1**.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2018 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2018 IG FISMA Metric Domains
Identify	Risk Management
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

The foundational levels of the maturity model focus on the development of sound, risk-based policies and procedures, while the advanced levels capture the institutionalization and effectiveness of those policies and procedures. **Table 2** explains the five maturity model levels. A functional information security area is not considered effective unless it achieves a rating of Level 4, *Managed and Measurable* or Level 5, *Optimized*.

[4] https://www.dhs.gov/publication/fy18-fisma-documents

Table 2: IG Evaluation Maturity Levels

Maturity Level	Maturity Level Description
Level 1: Ad hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Summary of Results

While PBGC continues to make progress in improving its information security and privacy program and its compliance with FISMA, OMB requirements, and applicable NIST guidance, its overall security program did not meet the requirements to be considered effective. Since last year, PBGC closed 12 out of 24 open recommendations reported in the FY 2017 FISMA audit, continued to implement technologies and processes to address long standing access controls and configuration management weaknesses. PBGC realizes it requires cycle time and institutional maturity to fully resolve these security weaknesses. Continued focus is needed by PBGC management to effectively remediate the remaining risks and weaknesses in the areas of risk management, and access and configuration management controls.

Current Results

Despite the noted progress, PBGC must make additional improvements to achieve an effective information security program. Specifically, CLA noted weaknesses in risk management, vulnerability and configuration management, identity and access management, data protection and privacy, security training, and information security continuous monitoring.

Our conclusions as to the effectiveness of PBGC's IT security incorporate multiple sets of test results, and are set forth below.

1. FISMA maturity scores

FISMA requires evaluators across the federal government to respond to 67 objective questions, from which a DHS algorithm calculates a maturity score for each of five functional areas. As set forth in the chart below, PBGC was rated at *Consistently Implemented* (Level 3) in four of the five functional areas. One functional area, *Respond*, was found to be *Managed and Measurable* (Level 4).[5] However, by these objective metrics, PBGC's overall security program fell below the minimum specified threshold of effective, which is level 4, *Managed and Measurable*.

Table 3 below summarizes the maturity ratings and assessment by function.

[5] The most frequent maturity level rating across the Protect function served as the overall Protect function rating.

Table 3: FY 2018 IG Cybersecurity Framework Domain Ratings

Cybersecurity Framework Security Functions[6]	Metric Domains	Calculated Maturity Level	Cyberscope Evaluation
Identify	**Risk Management**	Consistently Implemented (Level 3)	Not Effective
Protect	**Configuration Management**	Consistently Implemented (Level 3)	Not Effective
	Identity and Access Management	Consistently Implemented (Level 3)	Not Effective
	Data Protection and Privacy	Consistently Implemented (Level 3)	Not Effective
	Security Training	Defined (Level 2)	Not Effective
Detect	**Information Security Continuous Monitoring**	Consistently Implemented (Level 3)	Not Effective
Respond	**Incident Response**	Managed and Measurable(Level 4)	Effective
Recover	**Contingency Planning**	Consistently Implemented (Level 3)	Not Effective
Overall	**Not Effective**		

2. Detailed Findings

While PBGC has made progress in addressing the security weaknesses noted in prior years, work still remains to continue correcting these deficiencies. In this year's audit, we identified areas in the information security program that require strengthening. **Table 4** below summarizes our detailed findings.

[6] See Table 1 and Table 2 for definitions and explanations of the Cybersecurity Framework Security Functions and metric domains.

Table 4: Cybersecurity Framework Security Functions mapped to weaknesses noted in FY 2018 FISMA Assessment

FY 2018 IG FISMA Metric Domains	Weaknesses Noted in FY 2018
Risk Management	Security documentation was not consistently reviewed, approved, updated and uploaded into the official and authoritative repository for system authorization and risk management.
	Security assessment and authorization documentation were not completed, or completed timely.
	Systems in ongoing authorization did not have the correct, finalized, and up-to-date system security documentation recorded in the official tool.
	Plan of action and milestones were not established to mitigate risks identified in risk assessments.
	Lack of an insider threat detection and prevention program.
	Incomplete implementation of common security controls.
	Incomplete control implementation and assessment, and inadequate documentation of control inheritance[7] for the general support system.
Configuration Management	Ineffective patch and vulnerability management process for remediation of vulnerabilities.
	Remediation of vulnerabilities identified in key databases and applications not completed.
	Decommissioning of unsupported systems and databases not completed.
	Noncompliance with web server baseline configuration.
Identity and Access Management	Removal of terminated users' access by the effective separation date was not timely.
	Background reinvestigation weaknesses continued to exist during the fiscal year.
	Identified authentication weaknesses on systems.
Data Protection and Privacy	Some system technologies not upgraded or replaced to be compliant with encryption requirements.
	Project plans for data encryption has not been developed and implemented.
	Inadequate data loss prevention controls.
Security Training	New users did not complete the required security awareness training before being granted system access.
Information Security	Incomplete implementation of security information and event management tool.

[7] NIST SP 800-53, Revision 4, defines security control inheritance as "a situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides."

FY 2018 IG FISMA Metric Domains	Weaknesses Noted in FY 2018
Continuous Monitoring	Inadequate credential vulnerability scanning program.
	Inadequate data loss prevention controls.
	Network monitoring weaknesses.

Overall, we conclude that information security at PBGC has improved in a number of areas. With continued effort, attention, and investment, the information security program will mature and can cross the effectiveness threshold in the near future. At the present, however, the weaknesses that we identified leave PBGC operations and assets at risk of unauthorized access, misuse and disruption. To address these weaknesses, we made a total of 10 new, and 16 repeated or modified recommendations to assist PBGC in strengthening its information security program.

The following section provides a detailed discussion of the audit findings grouped by the Cybersecurity Framework Security Functions. Appendix A describes the audit scope and methodology.

FISMA Evaluation Findings

Security Function: Identify

Overview

PBGC developed and published the PBGC Risk Management Framework (RMF) process to fully implement its entity-wide information security risk management program. The RMF addresses both security and privacy controls. PBGC's IT risk management process focused on identifying and evaluating the threats and vulnerabilities to PBGC information. The RMF also focused on identifying risk management and mitigation strategies to address these threats and vulnerabilities. PBGC's risk management process still requires time to mature to be an effective continuous monitoring tool.

Metric Domain – Risk Management
Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact. With this information, organizations can determine the acceptable level of risk for delivery of services and can express this as their risk tolerance. NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems,* is guidance for implementing the risk management framework controls. The six step RMF includes security categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. The goal of the RMF is to provide near real-time risk management and ongoing authorization of information systems through robust continuous monitoring processes.

We identified the following information security weaknesses in the Risk Management domain:

- PBGC officials did not properly maintain current security documentation within the Cyber Security Assessment and Management system, PBGC's official and authoritative repository for system authorization and risk management. These security documents are required by PBGC policy to be uploaded to the Cyber Security Assessment and Management system any time a change is made or a document is created. The security documents support the initial authorization, reauthorization, and ongoing authorization reviews of PBGC's systems.

  PBGC did not consistently review, approve, update, and upload required system security documentation in its CSAM repository tool for several of its systems. For example, there was security assessment and authorization documentation that was not completed, or completed timely, based on the Enterprise Cybersecurity Division's FY 2018 Quarter 3 review of CSAM Quarterly Reviews for a selection of systems. Although the Security and Privacy Assessment & Authorization review identified documentation flaws, incomplete information, and missed reviews, the responsible parties were not correcting the identified items before expiration or need.

- PBGC's benefit payment system's interconnections inventory within CSAM and the System Security Plan did not include all system interconnections.

- In FY 2018, PBGC completed a Risk Assessment for the Information Technology Infrastructure Services General Support System. However, plans of action and milestones were not established to mitigate identified risks.

- PBGC has not implemented an insider threat detection and prevention program. NIST SP 800-53, Rev. 4, PM-12, *Insider Threat Program*, indicates that the organization is required to implement an insider threat program that includes a cross-discipline insider threat incident handling team. In 2017, PBGC delegated a senior PBGC official to be the responsible individual to implement and provide oversight for the insider threat program. In addition, during FY 2018, PBGC conducted exploratory discussions with other federal agencies on implementing an insider threat program. However, PBGC has not created a cross-discipline insider threat incident handling team.

- PBGC did not complete the implementation of NIST SP 800-53, Revision 4 controls that were designated as common controls,[8] remediate common controls weaknesses, and did not make the common controls available to system owners in CSAM for appropriate inclusion in their system security plans.

- The general support system owner did not complete the update of control implementation statements to reflect NIST SP 800-53, Revision 4; did not revise its inheritance of common controls; nor conduct an assessment of all controls in accordance with assessment schedules using NIST SP 800-53, Revision 4.

- PBGC's financial system had security controls that were applicable to the system, but were not implemented. In addition, plans of action and milestones were not established to track and monitor the implementation of these system controls.

Without effective risk management controls, PBGC is at risk of controls not operating as intended or not being implemented, increasing the likelihood of unauthorized modification, loss, and disclosure of critical and sensitive PBGC information.

Recommendations:

We recommend that PBGC improve the security of its environment by doing the following:

- Revise the processes and procedures of the continuous monitoring program to consistently enforce the review, update, and uploading of all required security assessment and authorization documentation for each system before the documentation expires. **(OIG Control Number FISMA-17-01)**

- Office of Benefits Administration should review and update their system interconnection inventories in accordance with PBGC *Office of Information Technology Interconnection Security Agreement Guidance*. **(OIG Control Number FISMA-18-01)**

[8] A common control is a security control that is inheritable by one or more organizational information systems.

- Office of Information Technology (OIT) should develop and implement procedures for the documentation of corrective actions within risk assessments. **(OIG Control Number FISMA-18-02)**

- OIT should update the Information Technology Infrastructure Services General Support System Risk Assessment to document corrective action plans. **(OIG Control Number FISMA-18-03)**

- PBGC should assign a senior organizational official responsible for, develop, and implement an insider threat detection and prevention program. **(OIG Control Number FISMA-16-14)**

- Complete the implementation of NIST SP 800-53, Revision 4 controls for common controls, remediation of common controls weaknesses and make available to system owners in Cyber Security Assessment and Management for appropriate inclusion in their system security plans. **(OIG Control Number FS-15-04)**

- Complete the update of control implementation statements to reflect NIST SP 800-53, Revision 4; revise the inheritance of common controls; and conduct an assessment of all controls in accordance with assessment schedules using NIST SP 800-53, Revision 4. **(OIG Control Number FISMA-17-02)**

- Control owners should ensure the creation of plans of action and milestones, and risks within the Risk Assessment for all controls not fully implemented to mitigate risks. The appropriate control provider should be identified to correct/mitigate the identified weakness. **(OIG Control Number FISMA-18-04)**

Security Function: Protect

Overview

In FY 2018, PBGC continued to implement technologies and processes to address long standing access controls and configuration management weaknesses. However, PBGC has realized it requires cycle time and institutional maturity to fully resolve some security weaknesses. Weaknesses in the PBGC IT environment continue to contribute to deficiencies in system configuration and access controls.

Metric Domain – Configuration Management
To secure both software and hardware, agencies must develop and implement standard configuration baselines that prevent or minimize exploitable system vulnerabilities. OMB requires all workstations that use Windows to conform to the U.S. Government Configuration Baseline standards. Furthermore, NIST has developed a repository of secure baselines for a wide variety of operating systems and devices.

CLA noted the following information security weaknesses in the Configuration Management domain:

- PBGC had an ineffective patch and vulnerability management process to remediate vulnerabilities identified in vulnerability assessment scans.
- PBGC has not completed the remediation of vulnerabilities identified in key databases and applications.
- PBGC did not complete the decommissioning of unsupported systems and databases.
- PBGC web servers were not in compliance with baseline configurations.

The details related to PBGC's vulnerability management program, patch management, and configuration management weaknesses were noted in the FY 2018 Vulnerability Assessment and Penetration Test Report, dated October 31, 2018. The following technical recommendations were issued in the restricted report: OIT-158R, OIT-160R, OIT-161R, OIT-164R, OIT-168R and OIT-169R.

Control weaknesses in the Configuration Management domain expose PBGC to increased risk of data compromise. Thus, PBGC may not have reasonable assurance regarding the confidentiality, integrity and availability of information in its systems.

Metric Domain – Identity and Access Management
Proper identity and access management ensures that users and devices are properly authorized to access information and information systems. Users and devices must be authenticated to ensure that they are who they identify themselves to be. In most systems, a user name and password serve as the primary means of authentication, and the system enforces authorized access rules established by the system administrator. To ensure that only authorized users and devices have access to a system, policy and procedures must be in place for the creation, distribution, maintenance, and eventual termination of accounts. Homeland Security Presidential

Directive 12 calls for all federal departments to require personnel to use personal identity verification cards. This use of personal identity verification cards is a major component of a secure, government-wide account and identify management system.

CLA noted the following information security weaknesses in the Identity and Access Management domain:

- PBGC did not complete the enhancements needed in its process for the timely removal of terminated users by the effective separation date. We continue to identify terminated users with active access to PBGC systems. The IT Infrastructure Operations Department worked in conjunction with the Workplace Solutions Department and the Quality Management Department to develop an updated separation process that would streamline tracking of separation actions, reduce manual steps, make reporting easier, and support compliance with their documented separation procedure. However, the updated separation process was recently implemented and therefore, there has not been enough cycle time to assess the effectiveness of the new process and continued improvements are needed to mitigate the deficiencies noted.

- PBGC continued to make progress with their background reinvestigation process. In FY 2018, the Human Resources Department Personnel & Physical Security Office substantially completed the initiation of background re-investigation for PBGC federal bargaining unit personnel as of September 30, 2018.

The details related to PBGC's vulnerability management program and authentication weaknesses were noted in the FY 2018 Vulnerability Assessment and Penetration Test Report, dated October 31, 2018. The following technical recommendations were issued in the restricted report: OIT-162R.

Control weaknesses in the Identity and Access Management domain expose PBGC to increased risk of data compromise. Thus, PBGC may not have reasonable assurance regarding the confidentiality and integrity of information in its systems.

Metric Domain – Data Protection and Privacy

FISMA requires the federal government to establish a privacy program and corresponding policies and procedures for the protection of personally identifiable information (PII) collected, used, maintained, shared, and disposed of by information systems. Training is to be provided for personnel responsible for PII or activities involving PII. In addition, agencies are required to develop a data breach response plan for reporting, investigating, and managing a privacy-related breach.

CLA noted the following information security weaknesses in the Data Protection and Privacy domain:

- A few of PBGC's system technologies require an upgrade or replacement to be compliant with encryption requirements as documented in FIPS 140-2, *Security Requirements for Cryptographic Modules* and OMB A-130, *Managing Information as a Strategic Resource*.

- PBGC has not developed and implemented project plans for satisfying data encryption recommendations made in their risk assessment.

The details related to PBGC's vulnerability management program, and data loss prevention weaknesses were noted in the FY 2018 Vulnerability Assessment and Penetration Test Report, dated October 31, 2018. The following technical recommendations were issued in the restricted report: OIT-167R.

Control weaknesses in the Data Protection and Privacy domain expose PBGC to increased risk of compromise of data confidentiality for millions of participants.

Metric Domain – Security Training

FISMA requires all federal government personnel and contractors to complete annual security awareness training that provides instructions on threats to data security and responsibilities in information protection. FISMA also requires specialized training for personnel and contractors with significant security responsibilities. Without adequate security training programs, agencies cannot ensure that personnel would have the knowledge required to ensure the security of the information systems and data.

CLA noted the following information security weaknesses in the Security Training domain:

- We continued to find new users did not complete required training (Security/Privacy Awareness training and rules of behavior) prior to being granted logical access during our review of access controls in FY 2018.

  PBGC transitioned to a new training system, FedTalent, as the old system, Talent Management System, was due to be decommissioned. PBGC has not had enough cycle time to fully implement FedTalent and update their policies and procedures to reflect the current operating environment at PBGC Headquarters, Field Benefit Administration sites and other PBGC locations.

Control weaknesses in the Security Training domain expose PBGC to increased risk of unintentional and insecure user behavior in protecting the technology environment. Thus, PBGC may not have reasonable assurance regarding the confidentiality and integrity of information in its systems.

Recommendations:

We recommend that PBGC improve the security of its environment by doing the following:

- Develop and implement plans of action for addressing known security weaknesses. **(OIG Control Number FS-16-08)**

- Document and implement enhanced processes and procedures to effectively track and remediate known vulnerabilities in a timely manner. **(OIG Control Number FISMA-17-03)**

- Implement controls to remedy vulnerabilities identified in key databases and applications, such as weaknesses in configuration, roles, privileges, auditing, file permissions, and operating system access. **(OIG Control Number FS-07-14)**

- Fully implement controls to plan, remove and decommission unsupported systems and databases. **(OIG Control Number FS-16-07)**

- PBGC should implement effective processes and procedures to ensure the secure configuration of web servers in accordance with the established configuration baselines and document deviations to the established baselines on an as needed basis. **(OIG Control Number FISMA-17-04)**

- Implement improved processes and provide training to ensure PBGC federal managers/Contracting Officer Representatives submit and approve separation requests prior (when applicable) to the effective separation date, as well as the collection of IT Assets by the effective separation date. **(OIG Control Number FS-18-12)**

- Implement improved processes and provide training to ensure PBGC Workplace Solutions Department removes physical access by the effective separation date. **(OIG Control Number FS-18-13)**

- Office of Benefits Administration should document enhanced account management procedures to ensure a thorough review of accounts is performed during the annual account recertification and that necessary accounts are recertified, and implement compensating controls to verify inactive accounts are deactivated in accordance with PBGC policy. **(OIG Control Number FS-17-05)**

- Develop, document, and implement a process for the timely assessment of employees and contractors transferred or promoted to a new position or role to determine whether the risk- level has changed. **(OIG Control Number FISMA-14-15)**

- Develop and implement plans for completing system technology upgrades or replacements to be compliant with FIPS 140-2 and OMB A-130. **(OIG Control Number FS-18-09)**

- Develop and implement project plans for satisfying the recommendations that were made in the *PBGC IT Infrastructure Operations Department Risk Based Encryption Assessment*, dated June 29, 2018, version 1.0. **(OIG Control Number FS-18-10)**

- Develop, document and implement new hire policies and procedures to reflect the current operating environment at PBGC headquarters, Field Benefit Administration sites and other PBGC locations. **(OIG Control Number FISMA-18-05)**

Security Function: Detect

Overview

In FY 2018, PBGC continued to enhance implementation of various tools and processes to detect threats and vulnerabilities to improve its continuous monitoring program. With the continued maturity and deeper implementation of these tools and processes, PBGC's continuous monitoring program is becoming more effective.

Metric Domain – Information Security Continuous Monitoring
The goal of Information Security Continuous Monitoring is to combat information security threats by maintaining ongoing awareness of information security, vulnerabilities, and threats to federal systems and information. Information Security Continuous Monitoring provides ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity posture, hygiene, and operational readiness.

CLA noted the following information security weaknesses in the Information Security Continuous Monitoring domain:

- PBGC did not complete its implementation of the security information and event management tool to fully maximize its capabilities. Specifically, the extension of the security information and event management capability to include coverage for PBGC's major applications had not been completed by PBGC system owners.[9]

- PBGC did not improve its credential[10] vulnerability scanning program to reduce the number of credential failures.

- PBGC did not implement adequate data loss prevention controls to address weaknesses in its perimeter defenses.

Control weaknesses in the Information Security Continuous Monitoring domain continue to expose PBGC to threats and vulnerabilities that could bypass its defenses, which may result in compromise and increased risk of unauthorized modification, loss, and disclosure of critical and sensitive PBGC information. Thus, PBGC may not have reasonable assurance regarding the confidentiality, integrity, and availability of information in its systems.

[9] NIST SP 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems define "*information system owner* [as] an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. The information system owner is responsible for addressing the operational interests of the user community (i.e., users who require access to the information system to satisfy mission, business, or operational requirements) and for ensuring compliance with information security requirements."
[10] The credentialed scan utilized a user ID and password to enumerate the locally installed software and identified vulnerabilities from the user perspective. The credentialed scan summarized risks and vulnerabilities associated with remote attacks that leverage actions by the user as in phishing attacks and browsing malicious web content.

Recommendations:

We recommend that PBGC improve the security of its environment by doing the following:

- Fully implement Splunk Enterprise in PBGC, including its security information and event management capability. **(OIG Control Number FISMA-15-01)**

- System Owners should conduct and document an analysis of major applications' critical auditable events and business transactions to identify audit logging needs and requirements. **(OIG Control Number FISMA-15-02)**

- System Owners should develop and implement plans to fully implement Splunk Enterprise for their major applications. **(OIG Control Number FS-07-17)**[11]

- PBGC should modify the *PBGC Cybersecurity and Privacy Catalog* and other PBGC policies to allow the designation of "AU-2 Audit Events and AU-2(3) Audit Events and Reviews and Updates" as a shared control between the Office of Information Technology and the System Owner or a system-specific control. **(OIG Control Number FS-18-11)**

- Perform scheduled credentialed scans to include all the systems and update PBGC policies and procedures to require regular credentialed scans. **(OIG Control Number FISMA-15-05)**

- Assess and document the adequacy of PBGC's current data loss prevention controls in place and determine if additional controls are needed based on cost and risk. **(OIG Control Number FS-14-12)**

[11] The audit recommendation wording for FISMA-15-02 and FS-07-17 was revised during FY 2018.

Security Function: Respond

Overview

In FY 2018, PBGC met its established timelines for responding to security incidents and followed its processes and procedures for handling incidents.

Metric Domain – Incident Response
Information security incidents occur on a daily basis. Agencies must have sound policies and planning in place to respond to these incidents and report them to the appropriate authorities. The United States Computer Emergency Readiness Team is to receive reports of incidents on unclassified Federal Government systems, and OMB requires the reporting of incidents that involve sensitive data, such as personally identifiable information, within strict timelines.

We did not find weaknesses in PBGC's Incident Response program.

Recommendations:

None.

Security Function: Recover

Overview

PBGC has an established process and program for testing its contingency plan. PBGC has an annual program to test its contingency plan and update the planning documents based on lessons learned from the test exercise.

Metric Domain – Contingency Planning

FISMA requires agencies to prepare for events that may affect an information resource's availability. This preparation requires identification of resources and risks to those resources, and the development of a plan to address the consequences if loss of a system's availability occurs. Consideration of risk to an agency's mission and the possible magnitude of harm caused by a resource's unavailability are key to contingency planning. NIST SP 800-34, Revision 1*, Contingency Planning Guide for Federal Information Systems*, defines contingency planning as "interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods." Once a contingency plan is established, training and testing must be conducted to ensure that the plan and individuals tasked with the contingency responsibilities will be capable in the event of an emergency.

PBGC has consistently implemented contingency planning processes but has not reached a level of maturity as defined by CyberScope metrics to be an effective overall program.[12] This is mainly because PBGC's contingency plan program has not addressed supply chain risks posed to its contingency plan program. In addition, PBGC does not collect metrics on the effectiveness of its information system contingency plans and related plans, such as organization and business process continuity, disaster recovery, incident management, insider threat implementation, and occupant emergency, as appropriate to deliver persistent situational awareness across PBGC. Although PBGC maturity was not effective in the Contingency Planning domain, we did not find weaknesses in PBGC's Contingency Planning program.

Recommendations:

None.

[12] A functional information security area is not considered effective unless it achieves a rating of Level 4, *Managed and Measurable* or Level 5, *Optimized*.

Appendix A: Scope and Methodology

Scope

CLA conducted this audit in accordance with performance auditing standards, as specified in the Government Accountability Office's *Government Auditing Standards*. Those standards require that the auditor plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for their findings and conclusions based on the audit objective.

The objective of this audit was to determine the extent to which PBGC's information security program and practices complied with FISMA requirements, DHS reporting requirements, and applicable OMB and NIST guidance.

CLA performed a vulnerability assessment and penetration test, and evaluated management, operational, and technical controls supporting major applications and general support system in accordance with NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.* The information security policies, procedures, and practices of the following PBGC systems were evaluated during FY 2018:

- Consolidated Financial System
- Trust Accounting System
- Premium and Practitioner System
- Pension Lump Sum Program
- Information Technology Infrastructure Services General Support System
- Spectrum

In addition, the audit included an assessment of effectiveness for each of the eight FY 2018 IG FISMA Metric Domains and the maturity level of the five Cybersecurity Framework Security Functions.

The audit also included a follow up on prior audit recommendations to determine if PBGC made progress in implementing the recommended improvements concerning its information security program.

Audit fieldwork was performed at PBGC's headquarters in Washington, D.C., during the period April 2018 through November 2018, at PBGC's headquarters in Washington, D.C.

Methodology

To accomplish the audit objective, CLA:

- Interviewed key personnel and reviewed legal and regulatory requirements stipulated by FISMA.
- Reviewed documentation related to PBGC's information security program, such as security policies and procedures, system security plans, security control assessments, risk assessments, security assessment authorizations, plan of action and milestones, incident response plan, configuration management plan, and continuous monitoring plan.
- Tested system processes to determine the adequacy and effectiveness of selected controls.

- Reviewed the status of recommendations in the prior year FISMA report, including supporting documentation to ascertain whether the actions taken addressed the weaknesses.

In addition, CLA assessed PBGC's technical controls by performing a network security test as part of the FISMA audit. The independent vulnerability assessment and penetration test was conducted to determine the effectiveness of internal controls that prevent and detect unauthorized access, disclosure, modification, or deletion of sensitive information. The results of the vulnerability assessment and penetration test was incorporated into our FISMA audit results.

To perform our review of PBGC's security program, we followed a work plan based on the following guidance:

- NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* for specification of security controls.
- NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems,* for the risk management framework controls.
- NIST SP 800-53A*,* Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations,* for the assessment of security control effectiveness.
- Government Accountability Office's (GAO) *Federal Information System Controls Audit Manual* (FISCAM: GAO-09-232G), for the information technology audit methodology.

In testing for the adequacy and effectiveness of the security controls, CLA exercised professional judgment in determining the number of items selected for testing and the method used to select them. Relative risk and the significance or criticality of the specific items in achieving the related control objectives was considered. In addition, the severity of a deficiency related to the control activity and not the percentage of deficient items found compared to the total population available for review was considered. In some cases, this resulted in selecting the entire population. However, in cases where an entire audit population was not selected, the results cannot be projected and if projected may be misleading.

Appendix B: Status of Prior-Year Recommendations

The following is the status of outstanding recommendations not included in the report and PBGC's plans for corrective action. As noted in the table below, some recommendations remain in progress, with estimated completion dates still to be determined. The corrective actions outlined below are based on management assertions and results of our audit.

FISMA Recommendations Closed in Fiscal Year 2018

OIG Control Number	Date Closed	Original Report Number
FISMA-16-03	October 10, 2018	EVAL 2017-9 /FA-16-110-7
FISMA-16-04	October 23, 2018	EVAL 2017-9 /FA-16-110-7
FISMA-16-05	August 31, 2018	EVAL 2017-9 /FA-16-110-7
FISMA-16-08	September 24, 2018	EVAL 2017-9 /FA-16-110-7
FISMA-16-10	October 23, 2018	EVAL 2017-9 /FA-16-110-7
FISMA-16-11	October 23, 2018	EVAL 2017-9 /FA-16-110-7
FISMA-16-12	October 23, 2018	EVAL 2017-9 /FA-16-110-7
FISMA-16-15	October 17, 2018	EVAL 2017-9 /FA-16-110-7
FISMA-16-16	November 6, 2108	EVAL 2017-9 /FA-16-110-7
FISMA-16-17	October 17, 2018	EVAL 2017-9 /FA-16-110-7
FISMA-16-18	October 17, 2018	EVAL 2017-9 /FA-16-110-7
FISMA-16-19	October 17, 2018	EVAL 2017-9 /FA-16-110-7

Prior and Current Years' Open FISMA Recommendations in Fiscal Year 2018

OIG Control Number	Original Report Number
Prior Year	
FISMA-14-15	EVAL-2015-9/FA-14-101-7
FISMA-15-01	EVAL-2016-7/FA-15-108-7
FISMA-15-02	EVAL-2016-7/FA-15-108-7
FISMA-15-05	EVAL-2016-7/FA-15-108-7
FS-07-17	2008-2/FA-0034-2
FS-14-12	AUD-2015-3/FA-14-101-3
FISMA-16-14	EVAL-2017-9 /FA-16-110-7
FS-15-04	AUD-2016-3/FA-15-108-3
FS-07-14	2008-2/FA-0034-2
FS-16-07	AUD-2017-3/FA-16-110-2
FS-16-08	AUD-2017-3/FA-16-110-2
FS-17-05	AUD-2018-6/FA-17-19-3
FISMA-17-01	EVAL-2018-7/FA-17-119-6
FISMA-17-02	EVAL-2018-7/FA-17-119-6
FISMA-17-03	EVAL-2018-7/FA-17-119-6
FISMA-17-04	EVAL-2018-7/FA-17-119-6

OIG Control Number	Original Report Number
Current Year	
FISMA-18-01	
FISMA-18-02	
FISMA-18-03	
FISMA-18-04	
FISMA-18-05	
FS-18-09	AUD-2019-1/FA-18-127-1
FS-18-10	AUD-2019-1/FA-18-127-1
FS-18-11	AUD-2019-1/FA-18-127-1
FS-18-12	AUD-2019-1/FA-18-127-1
FS-18-13	AUD-2019-1/FA-18-127-1

Appendix C: Management Comments

PBGC
Protecting America's Pensions
Pension Benefit Guaranty Corporation
1200 K Street, N.W., Washington, D.C. 20005-4026

Office of the Director

DEC 17 2018

To: Robert A. Westbrooks
Inspector General

From: W. Thomas Reeder

Subject: Response to OIG's Draft Fiscal Year 2018 FISMA Report

Thank you for the opportunity to comment on the Office of Inspector General (OIG's) draft report, dated December 4, 2018, relating to FY 2018 compliance with the Federal Information Security Management Act (FISMA). Your office's work on this is sincerely appreciated.

It was helpful to receive the associated Notices of Findings and Recommendations (NFRs) ahead of this report. This allowed for expeditious initiation of planning and remediation activities, which will lead to mutually desirable outcomes for the agency and the OIG.

Management is in agreement with the report's findings and recommendations. In the attachment to this report, you will find our specific responses to each recommendation included in the report, as well as our planned corrective actions and scheduled completion dates. Addressing these recommendations in a timely manner is an important priority for PBGC.

Attachment

cc: Patricia Kelly, Chief Financial Officer
David Foley, Chief of Benefits Administration
Alice Maroni, Chief Management Officer
Karen Morris, Acting Chief of Negotiations and Restructuring
Michael Rae, Deputy Chief Policy Officer
Robert Scherer, Chief Information Officer
Judith Starr, General Counsel
Marty Boehm, Director, Corporate Controls and Reviews Department

ATTACHMENT

Our comments on the specific recommendations in the draft report are as follows:

1. FISMA-18-01 Office of Benefits Administration should review and update their system interconnection inventories in accordance with PBGC *Office of Information Technology Interconnection Security Agreement Guidance*.

PBGC Response: PBGC agrees with this recommendation. ECD has already begun work to address the recommendation under POA&M 2792.

Scheduled Completion Date: June 30, 2019

2. FISMA-18-02 Office of Information Technology (OIT) should develop and implement procedures for the documentation of corrective actions within risk assessments.

PBGC Response: PBGC agrees with this recommendation. ITIOD will address documentation of corrective actions within the Risk Management Framework.

Scheduled Completion Date: June 30, 2020

3. FISMA-18-03 OIT should update the Information Technology Infrastructure Services General Support System Risk Assessment to document corrective action plans.

PBGC Response: PBGC agrees with this recommendation. ITIOD will address documentation of corrective actions within the Risk Management Framework. ITIOD will use the documentation of corrective actions within the Risk Management Framework for the ITISGSS.

Scheduled Completion Date: June 30, 2020

4. FISMA-18-04 Control owners should ensure the creation of plans of action and milestones, and risks within the Risk Assessment for all controls not fully implemented to mitigate risks. The appropriate control provider should be identified to correct/mitigate the identified weakness.

PBGC Response: PBGC agrees with this recommendation. ECD and FOD are collaborating to ensure the identified controls are appropriately implemented.

Scheduled Completion Date: June 30, 2019

5. FISMA-18-05 Develop, document, and implement new hire policies and procedures to reflect the current operating environment at PBGC headquarters, Field Benefit Administration sites, and other PBGC locations.

PBGC Response: PBGC agrees with this recommendation. ITIOD will document New Hire policies and procedures to reflect the current operating environment at PBGC headquarters, FBA sites, and other PBGC locations.

Scheduled Completion Date: June 30, 2019